

EXHIBIT 16

U.S. Patent No 9,100,431 v. Zoho

Overview

Plaintiff accuses Defendant of infringement through making, using, selling, offering for sale and importation of the Zoho's ("Defendant" or "Zoho") ManageEngine, including Endpoint Central and Vulnerability Manager Plus (the "Accused System and Method"), and all substantially similar products. The term "Accused System and Method" includes the associated computer hardware, interfaces, software and data, and the processes and methods related thereto.

The Accused System and Method is accused of directly infringing U.S. Patent No. 9,100,431 (the "'431 Patent"). Plaintiff further accuses Defendant of indirectly infringing the '431 Patent by providing its customers and others the Accused System and Method to utilize in an infringing manner. Defendant intends to cause infringement by its customers and users as Defendant instructs users to use the Accused System and Method in an infringing manner. Defendant deploys client software to implement the Accused System and Method. Defendant also provides support and implementation services for the Accused System and Method, including providing instructions, guides, online materials and technical support.

The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of Defendant's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff. Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports.

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**




9,100,431 Claim 14	Evidence
<p>14. (Not presently asserted but intervening for asserted claims 19 and 20) A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:</p>	<p>ManageEngine includes <i>a computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:</i></p> <p>Note: See, for example, the evidence below (emphasis added, if any):</p> <div data-bbox="758 553 1719 1274"> <div data-bbox="758 553 1719 631"> Enterprise vulnerability management software </div> <div data-bbox="827 631 1705 915"> <p>Vulnerability Manager Plus is a multi-OS vulnerability management and compliance solution that offers built-in remediation. It is an end-to-end vulnerability management tool delivering comprehensive coverage, continual visibility, rigorous assessment, and integral remediation of threats and vulnerabilities, from a single console. Whether your endpoints are on your local network, in a DMZ (demilitarized zone) network, at a remote location, or on the move, Vulnerability Manager Plus is the go-to solution to empower your distributed workforce with safe working conditions. Learn how to perform step-by-step vulnerability management in your enterprise with Vulnerability Manager Plus.</p> </div> <div data-bbox="726 964 856 1143"> <p>Scan</p>  </div> <div data-bbox="617 1187 974 1274"> <p>Scan and discover exposed areas of all your local and remote office endpoints as well as roaming devices.</p> </div> <div data-bbox="1215 964 1310 1143"> <p>Assess</p>  </div> <div data-bbox="1100 1187 1430 1274"> <p>Leverage attacker-based analytics, and prioritize areas that are more likely to be exploited by an attacker.</p> </div> <div data-bbox="1677 964 1787 1143"> <p>Manage</p>  </div> <div data-bbox="1551 1187 1923 1274"> <p>Mitigate the exploitation of security loopholes that exist in your network and prevent further loopholes from developing.</p> </div> </div>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

	<p>https://www.manageengine.com/vulnerability-management/?pos=EndpointCentral&loc=ProdMenu&cat=UEMS</p> <p>Comprehensive vulnerability scanning</p> <p>Eliminating blind spots is the basis of successful vulnerability management. To achieve this, Vulnerability Manager Plus:</p> <ul style="list-style-type: none"> • Detects known or emerging vulnerabilities across all your network endpoints, including workstations, laptops, servers, web servers, databases, virtual machines, and content management systems. • Offers continuous visibility into your endpoints, whether they are located at the local office, in a demilitarized zone, at a remote location, or always on the move. • Extends your visibility beyond just vulnerabilities and identifies misconfigurations, high-risk software, active ports, and much more. <p>https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html</p>
<p>code for:</p> <p>accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take</p>	<p>ManageEngine includes code for: <i>accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities</i> (e.g., a Central Vulnerability Database) <i>each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option</i> (e.g., threats, patches, vulnerabilities, and compliance policies, etc. for mitigate effects of attacks).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

Vulnerability Manager Plus Server:

The Vulnerability Manager Plus Server helps you to centrally perform all the vulnerability management and compliance tasks in your network endpoints. Some of the tasks include the following:

- Installing agents in computers
- Scanning computers for vulnerabilities and misconfigurations
- Deploying patches and secure configurations
- Uninstalling high-risk software
- Auditing active ports
- Auditing for compliance against CIS benchmarks

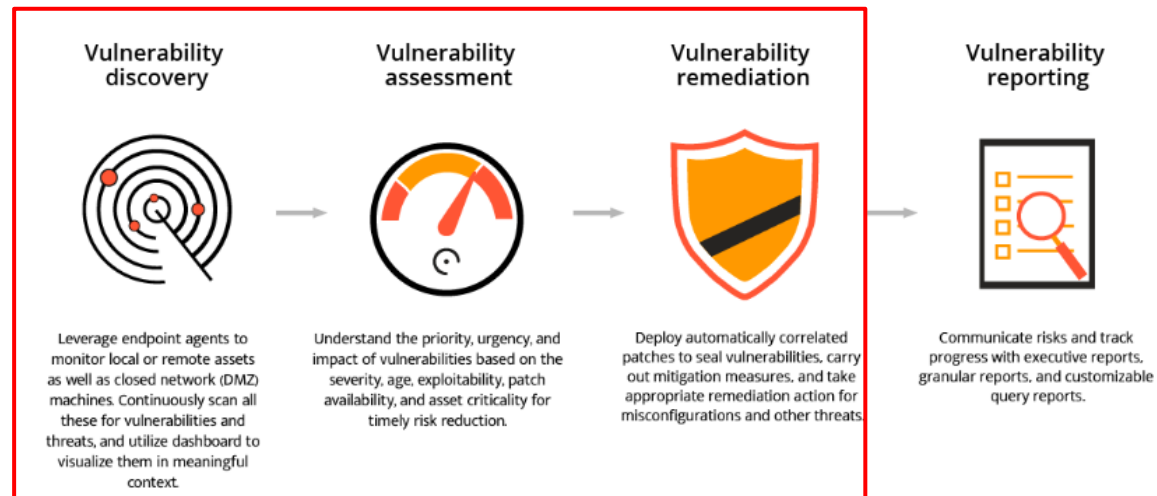
Any of the Windows computers in your network with the requirements mentioned [here](#) can be hosted as your Vulnerability Manager Plus Server. This Vulnerability Manager Plus Server at the customer site subscribes to the Central Vulnerability Database, from which it synchronizes the latest information on threats, patches, vulnerabilities, and compliance policies. Patches are downloaded directly from vendor sites and stored centrally in the server's patch store and will be replicated to your network endpoints to conserve bandwidth.

<https://www.manageengine.com/vulnerability-management/help/vulnerability-management-architecture.html#v1>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****All-in-one platform for vulnerability scanning and more!**

Scanning for vulnerabilities, system misconfigurations and other security loopholes in the network isn't enough, if those aren't mitigated promptly. This is where Vulnerability Manager Plus stands out. By leveraging the agents installed in the systems, this solution combines vulnerability scanning, patch deployment, security configuration management, and other mitigation strategies together into a single console. This shortens the time taken to detect and remediate vulnerabilities and misconfigurations.

With Vulnerability Manager Plus, you only need one tool and one agent to manage all your system vulnerabilities. This means it's easy to use in changing environments and you don't have to waste time scanning multiple times for the same issues. The tool automatically gathers all the important information and helps you quickly fix any problems.



<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

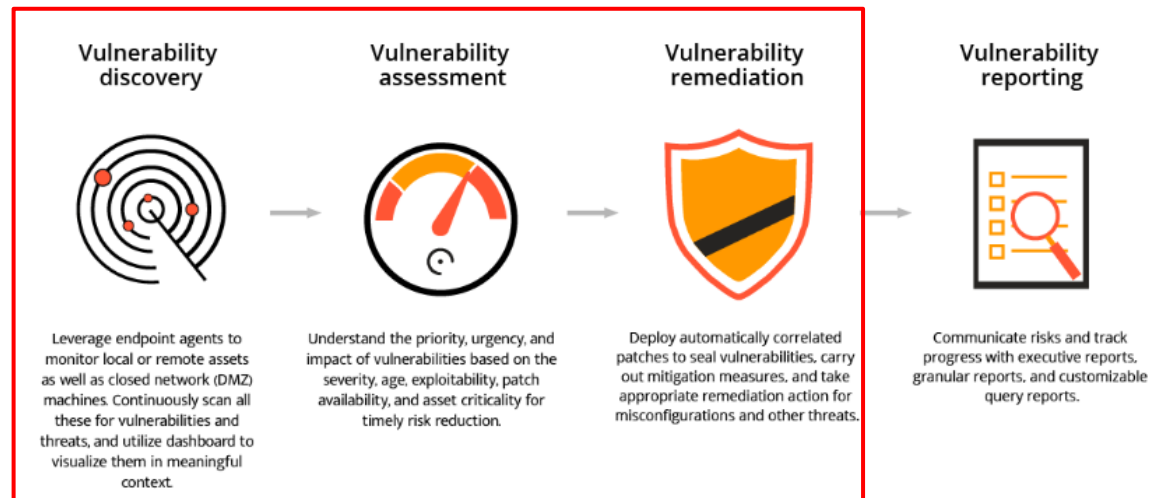
EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

code for: receiving information in connection with at least one of a plurality of devices; and identifying an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information;	ManageEngine includes code for: <i>receiving information in connection with at least one of a plurality of devices</i> (e.g., a Vulnerability Scanner) <i>identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability, based on the information</i> (e.g., Vulnerability Manager Plus features a agents installed on systems to integrate vulnerability scanning, patch deployment, security configuration management, and various mitigation strategies into a single unified console). Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):
--	---

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****All-in-one platform for vulnerability scanning and more!**

Scanning for vulnerabilities, system misconfigurations and other security loopholes in the network isn't enough, if those aren't mitigated promptly. This is where Vulnerability Manager Plus stands out. By leveraging the agents installed in the systems, this solution combines vulnerability scanning, patch deployment, security configuration management, and other mitigation strategies together into a single console. This shortens the time taken to detect and remediate vulnerabilities and misconfigurations.

With Vulnerability Manager Plus, you only need one tool and one agent to manage all your system vulnerabilities. This means it's easy to use in changing environments and you don't have to waste time scanning multiple times for the same issues. The tool automatically gathers all the important information and helps you quickly fix any problems.



<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install Patch' configuration screen in the ManageEngine Vulnerability Management console. The interface includes a sidebar with navigation options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agent', 'Reports', 'Admin', and 'Support'. The main content area is titled 'Install (Universal) Windows Patch (Computer)' and contains several sections:

- Name and Description:** A text input field with 'MSConfiguredP02' and an 'Add Description' link.
- Install Patch:** A section with 'Operate Type' set to 'Install Patch' and a table of patches.
- Schedule Settings (optional):** Checkboxes for 'Install Once' and 'Do not apply this configuration after the time specified below'.
- Deployment Rule:** A checkbox for 'Continue deployment even if some patches cannot be downloaded'.
- Deployment Settings:** A dropdown for 'Apply Deployment Policy' set to 'Select Policy' and a 'Create New Policy' link.
- Define Target:** A section for selecting targets, with 'Remote Office Domain' and 'Local Office' options.
- Execution Settings (Optional):** A section for defining execution settings.

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
10300	Security Update for Windows 8.1 KB3033780	Not Required	Security Update	Approved	1	0	X
10304	Security Update for Windows 8.1 KB3033782	Not Required	Security Update	Approved	1	0	X

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

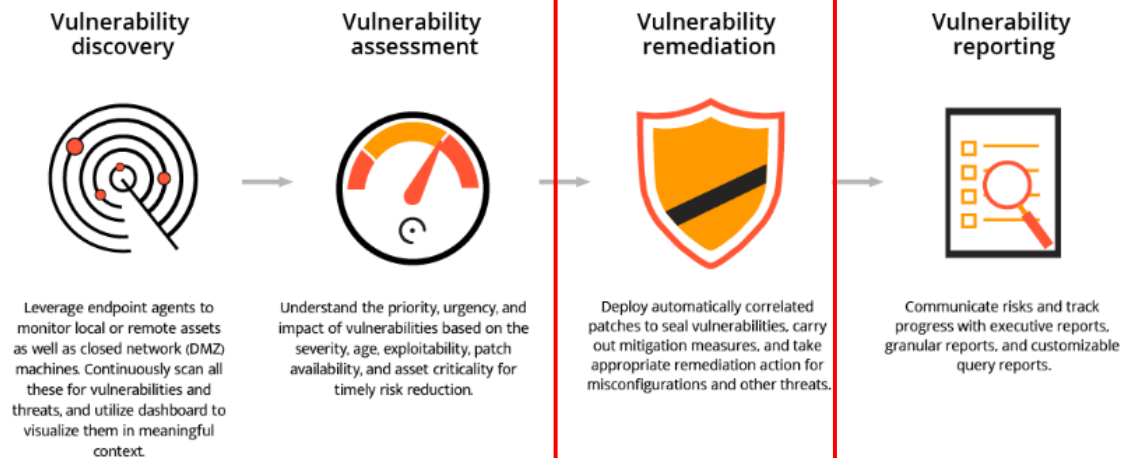
EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

<p>code for:</p> <p>automatically applying at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device, for mitigating an effect of the attack on the at least one device that takes advantage of the at least one vulnerability;</p>	<p>ManageEngine includes code for: <i>automatically applying at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device, for mitigating an effect of the attack on the at least one device that takes advantage of the at least one vulnerability</i> (e.g., Vulnerability Manager Plus features a agents installed on systems to integrate vulnerability scanning, automatic patch deployment, security configuration management, and various mitigation strategies into a single unified console).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>
---	--

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****All-in-one platform for vulnerability scanning and more!**

Scanning for vulnerabilities, system misconfigurations and other security loopholes in the network isn't enough, if those aren't mitigated promptly. This is where Vulnerability Manager Plus stands out. By leveraging the agents installed in the systems, this solution combines vulnerability scanning, patch deployment, security configuration management, and other mitigation strategies together into a single console. This shortens the time taken to detect and remediate vulnerabilities and misconfigurations.

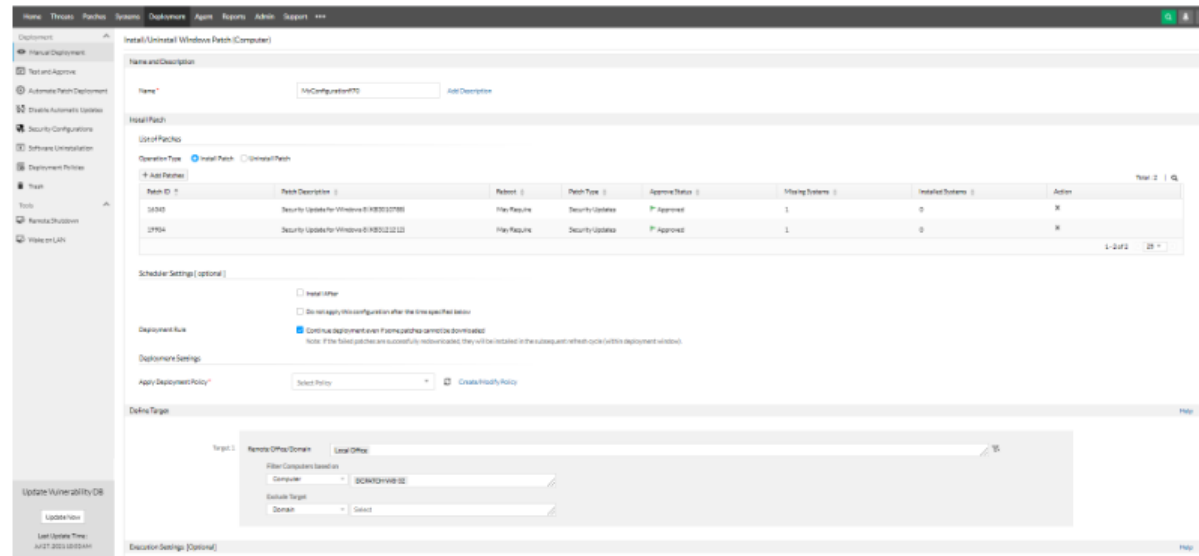
With Vulnerability Manager Plus, you only need one tool and one agent to manage all your system vulnerabilities. This means it's easy to use in changing environments and you don't have to waste time scanning multiple times for the same issues. The tool automatically gathers all the important information and helps you quickly fix any problems.



<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.



<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

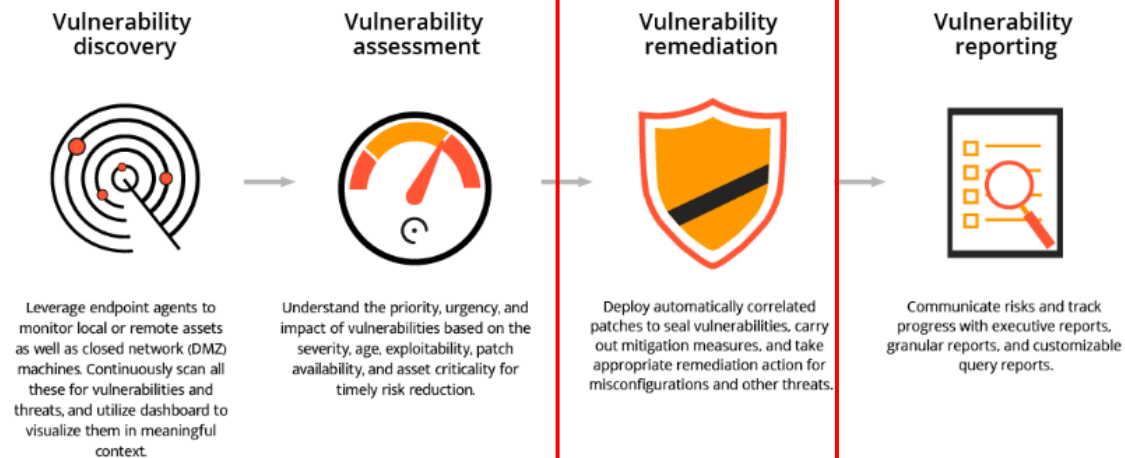
EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

wherein the computer program product is operable such that the effect of the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability;	<p>ManageEngine includes <i>computer program product is operable such that the effect of the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability</i> (e.g., Vulnerability Manager Plus features a agents installed on systems to integrate vulnerability scanning, automatic patch deployment, security configuration management, and various mitigation strategies into a single unified console).</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p>
--	---

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****All-in-one platform for vulnerability scanning and more!**

Scanning for vulnerabilities, system misconfigurations and other security loopholes in the network isn't enough, if those aren't mitigated promptly. This is where Vulnerability Manager Plus stands out. By leveraging the agents installed in the systems, this solution combines vulnerability scanning, patch deployment, security configuration management, and other mitigation strategies together into a single console. This shortens the time taken to detect and remediate vulnerabilities and misconfigurations.

With Vulnerability Manager Plus, you only need one tool and one agent to manage all your system vulnerabilities. This means it's easy to use in changing environments and you don't have to waste time scanning multiple times for the same issues. The tool automatically gathers all the important information and helps you quickly fix any problems.



<https://www.manageengine.com/vulnerability-management/vulnerability-scanner.html>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install Patch' configuration page in the ManageEngine Vulnerability Management interface. The page is titled 'Install (Universal) Windows Patch (Computer)' and includes a sidebar with navigation options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agent', 'Reports', 'Admin', and 'Support'.

Name and Description: The 'Name' field is set to 'MSConfiguredP02'.

Install Patch: The 'Operation Type' is set to 'Install Patch'. Below this is a table listing patches:

Patch ID	Patch Description	Reboot	Patch Type	Approval Status	Missing Systems	Installed Systems	Action
16300	Security Update for Windows 8.1 KB3033780	Yes/Require	Security Update	Approved	1	0	X
16304	Security Update for Windows 8.1 KB3033782	Yes/Require	Security Update	Approved	1	0	X

Scheduler Settings (optional): Includes checkboxes for 'Install on first' and 'Do not apply this configuration after the time specified below'. The 'Deployment Rule' is set to 'Continue deployment even if some patches are not installed'.

Deployment Settings: The 'Apply Deployment Policy' dropdown is set to 'Select Policy', with a 'Create New Policy' link.

Define Target: The 'Target' is set to 'Remote Office Domain'. The 'Filter Computers based on' dropdown is set to 'Computer', and the 'Domain' is set to 'BCHWTCORP02'.

Execution Settings (Optional): This section is currently collapsed.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

<p>wherein the computer program product is operable such that one or more of the plurality of mitigation techniques is identified based on an identification of an operating system.</p>	<p>ManageEngine includes a <i>computer program product that is operable such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system</i> (e.g., Vulnerability Manager Plus deploy mitigation techniques to different operating system)</p> <p>Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):</p> <p>You can set up distribution servers, which replicate primary server commands, for your remote offices simplify management and conserve bandwidth. You can even manage assets within a closed network like a DMZ.</p> <p>Identified systems are probed for different attributes: operating systems, open ports, installed software, user accounts, file system structure, system configurations, and more. Using the library of up-to-date scan data, Vulnerability Manager Plus checks the discovered assets for threats and vulnerabilities and delivers appropriate remediation.</p> <p>Generally, patches are downloaded directly from vendor sites, stored centrally in the server's patch store, and replicated to your network endpoints to conserve bandwidth. For remote workers, you can have the client machines download essential patches from trusted vendor sites without bottlenecking the limited bandwidth of the VPN gateways.</p> <p>The web console is the heart of vulnerability management. It allows you to monitor your security posture and carry out all tasks anywhere, anytime.</p> <p>https://www.manageengine.com/vulnerability-management/what-is-vulnerability-management.html</p>
--	---

EXHIBIT 16

U.S. Patent No 9,100,431 v. Zoho

| How to automate your organization's patch management schedule?

It's safe to assume that vulnerabilities are a constant threat to the network. Manual intervention is required to accurately assess and address the high profile vulnerabilities consistently. But given the rate at which new vulnerabilities surface, manually it's both easy to overlook certain critical vulnerabilities, as well difficult to reduce the total number of unpatched vulnerabilities in your network.

While you focus on what matters the most, let Vulnerability Manager Plus' built-in patching module regularly clean up the vulnerabilities in your network by automating the entire cycle of patching—including missing patch detection, download, testing, and deployment—to Windows, Mac, Linux, and over 300 third-party applications. The comprehensive patching functionality enables you to choose the criteria of patches to be automated, specific target machines/custom groups to be patched, flexible deployment policies, patch testing, and approval as well as deployment schedules based on your business requirements. What's more, you can use pre-built Patch Tuesday-based deployment policies to synchronize your patching with monthly Patch Tuesdays, and more. Explore the exhaustive capabilities of Vulnerability Manager Plus' [automated patch management](#).

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment-process.html>

EXHIBIT 16

U.S. Patent No 9,100,431 v. Zoho




	Features of ManageEngine's vulnerability management tool		
	<div>Vulnerability assessment<p>Identify real risks from a plethora of vulnerabilities.</p><p>Assess and prioritize vulnerabilities based on exploitability, severity, age, affected system count, as well as the availability of the fix.</p></div>	<div>Compliance<p>Meet security and audit objectives</p><p>Audit and maintain your systems in line with 75+ CIS benchmarks, instantly identify violations, view detailed remediation insights.</p></div>	<div>Patch management<p>Customize, orchestrate, and automate your entire patching process.</p><p>Download, test, and deploy patches automatically to Windows, Mac, Linux, and over 500 third-party applications with an integral patching module—at no additional cost.</p></div>
https://www.manageengine.com/vulnerability-management/			

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

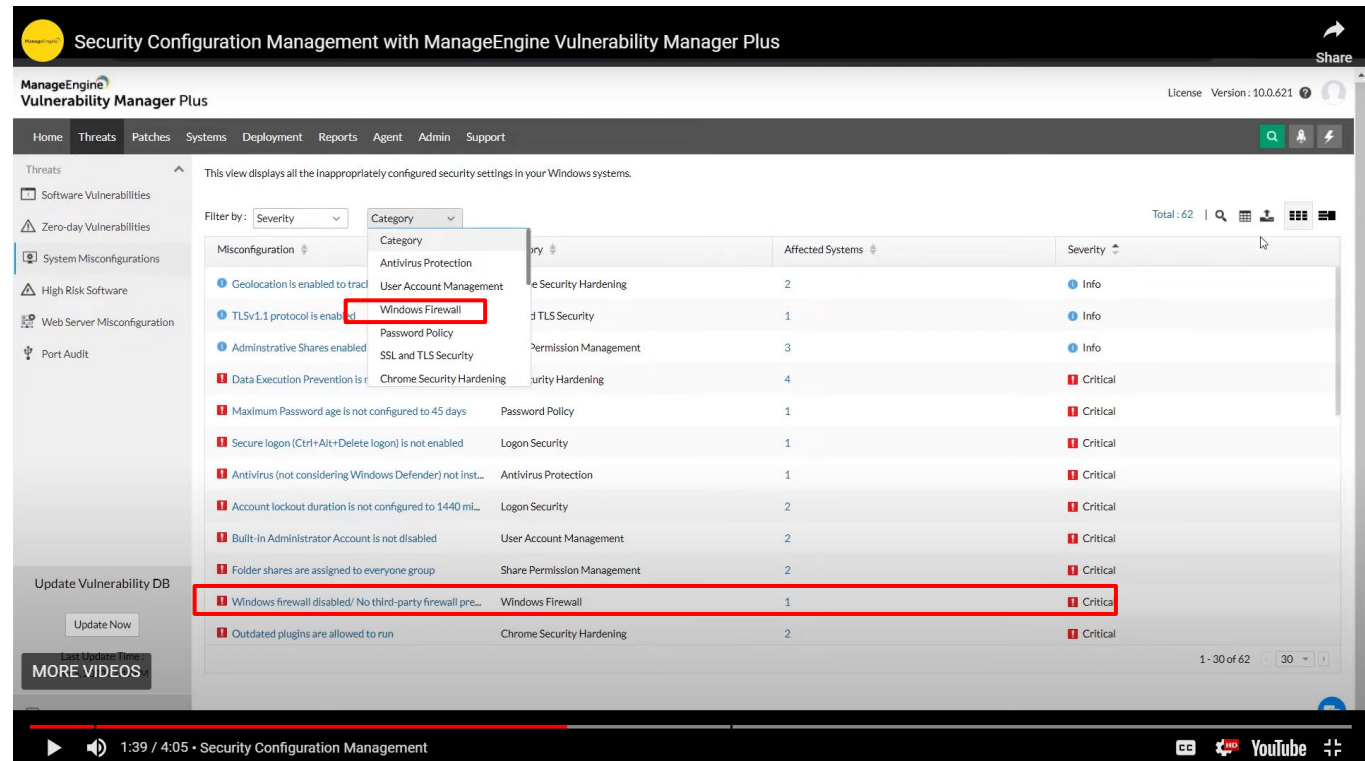
	<p>Automated patch deployment:</p> <p>Achieve cradle to grave automation in patching right from detecting missing patches in all the endpoints, downloading them respective vendors, testing them out for stability till deploying them to production machines.</p> <ul style="list-style-type: none"> • Keep abreast of frequent release of patches from multiple vendors. • Schedule scans by time, computer, group or user-defined collections of computers and continuously monitor missing patches on the endpoints. • Select the criteria of patches you wish to deploy and select target machines/ groups for your deployment, and let patch management takes care of everything else. • Gain Periodic updates on patch deployment status and redeploy failed patches without having to lift a finger. <p>https://www.manageengine.com/vulnerability-management/patch-management.html</p>
9,100,431 Claim 19	Evidence
19. The computer program product of claim 14, wherein the computer program product is operable such that the at least one first mitigation technique of the	<p>ManageEngine includes a <i>computer program product is operable such that the at least one first mitigation technique of the first mitigation type</i> (e.g., ManageEngine Vulnerability Manager Plus includes firewall option), <i>and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by a same system component that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied</i> (e.g., ManageEngine Vulnerability</p>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

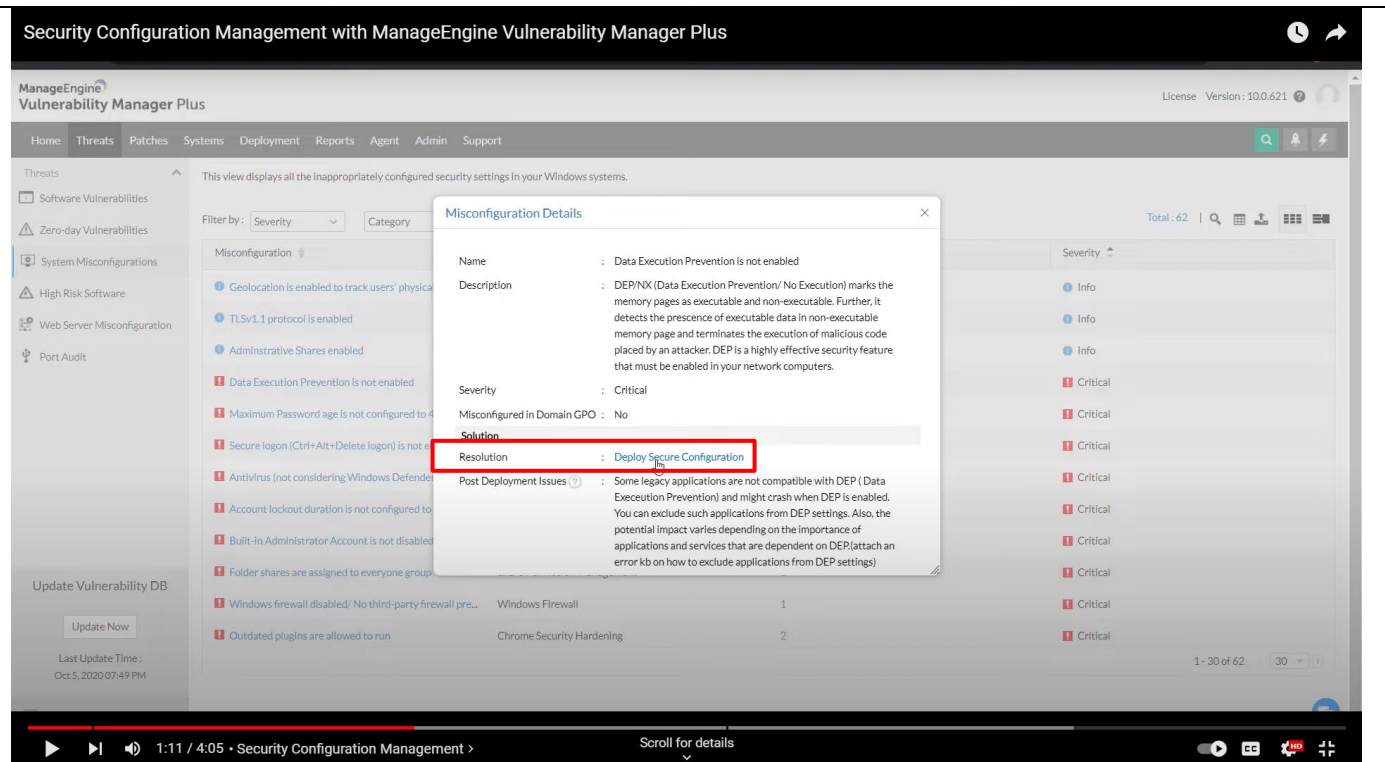
first mitigation type and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by a same system component that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied.

Manager Plus includes antivirus option). ManageEngine Vulnerability Manager Plus provides the option to deploy patches and configuration from the central dashboard.

Note: See, for example, the evidence above (where applicable) and below (emphasis added, if any):



<https://www.youtube.com/watch?v=p2Oh87NruMo>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho**

<https://www.youtube.com/watch?v=p2Oh87NruMo>

EXHIBIT 16

U.S. Patent No 9,100,431 v. Zoho

Firewall Policy Management

Firewall Analyzer is a firewall administration software, that helps in administering firewall rules and policies into multiple firewalls. The firewall rule automation ensures that firewall rules are pushed into the device seamlessly, avoiding errors and oversight. This firewall administration tool is capable of making the following changes.

- Add, modify, and delete network and service objects
- Add, modify, and delete firewall rules
- Analyze the implications of proposed firewall rule changes
- Push changes directly to the firewall

Refer the '[Firewall Rule Administration](#)' page for more details.

Firewall Analyzer is an efficient firewall rule and policy management tool that helps you gain visibility on all firewall rules, optimize firewall rules, and remove rule anomalies. It provides rule management reports for [most major firewall devices](#) including [Cisco](#), [FortiGate](#), [WatchGuard](#), and [Check Point](#).

<https://www.manageengine.com/products/firewall/firewall-rule-management.html>

EXHIBIT 16**U.S. Patent No 9,100,431 v. Zoho****Leverage built-in patching to ensure swift and accurate remediation**

With the built-in patching functionality automatically correlating patches with corresponding vulnerabilities, you can deliver instant remediation to all affected machines directly. Not only can you decide when patching should begin and end, but you can also customize every aspect of your patching process using flexible deployment policies. Affected target systems are automatically listed; here, you can add or remove targets as desired. You can also retry patch deployments on failed targets as many times as you want and choose to be notified about the deployment status at a frequency of your choosing.

The screenshot displays the 'Install Patch' configuration interface in the ManageEngine Vulnerability Management console. The interface includes a sidebar with navigation options like 'Home', 'Threats', 'Patches', 'Systems', 'Deployment', 'Agent', 'Reports', 'Admin', and 'Support'. The main content area is titled 'Install (Universal) Windows Patch (Computer)' and contains the following sections:

- Name and Description:** A text field for 'Name' (containing 'MSConfiguredP02') and a link for 'Add Description'.
- Install Patch:** A section for selecting patches to install. It includes a table with columns: Patch ID, Patch Description, Patch Type, Patch Type, Approval Status, Missing Systems, Installed Systems, and Action. Two patches are listed: 'KB3033920' and 'KB3033921', both with a status of 'Approved' and 1 missing system.
- Schedule Settings (optional):** Checkboxes for 'Install Once' and 'Do not apply this configuration after the time specified below'. The 'Do not apply' checkbox is checked.
- Deployment Rule:** A checkbox for 'Continue deployment even if patches cannot be downloaded'.
- Deployment Settings:** A dropdown for 'Apply Deployment Policy' (set to 'Select Policy') and a link for 'Create New Policy'.
- Define Target:** A section for selecting target systems. It includes a 'Target' dropdown (set to 'Remote Office/Domain'), a 'Filter Computers based on' dropdown (set to 'Computer'), and a 'Domain' dropdown (set to 'BOWINGHUB-02').
- Execution Settings (Optional):** A section for configuring execution settings.

<https://www.manageengine.com/vulnerability-management/vulnerability-assessment.html>

EXHIBIT 16

U.S. Patent No 9,100,431 v. Zoho

| Test and approve patches:

- Create a test group that is identical to the production environment.
- Automatically test patches for for incompatibility, unintended bugs or any other installation failure issues.
- Once tested, you can choose to approve patches either manually or automatically.
- Successfully tested and approved patches will be taken up for Automated Patch Deployment tasks.

| Automated patch deployment:

Achieve cradle to grave automation in patching right from detecting missing patches in all the endpoints, downloading them respective vendors, testing them out for stability till deploying them to production machines.

- Keep abreast of frequent release of patches from multiple vendors.
- Schedule scans by time, computer, group or user-defined collections of computers and continuously monitor missing patches on the endpoints.
- Select the criteria of patches you wish to deploy and select target machines/ groups for your deployment, and let patch management takes care of everything else.
- Gain Periodic updates on patch deployment status and redeploy failed patches without having to lift a finger.

<https://www.manageengine.com/vulnerability-management/patch-management.html>